Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 19, 2019

2. Name of company(s) covered by this certification: K & M Telephone Company, Inc.

3. Form 499 Filer ID: 801270

4. Name of signatory: Thomas A. Magnuson

5. Title of signatory: President/GM

6. Certification:

I, Thomas A. Magnuson, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachment: Accompanying Statement explaining CPNI procedures

POLICY FOR COMPLIANCE WITH CPNI RULES

K & M Telephone Company, Inc. (here-in-after the "Corporation") implements the following policy to ensure that the Corporation is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information ("CPNI"), § 64.2001 through § 64.2011. The purpose of the policy is to safeguard customer information.

Definition of CPNI

CPNI is the information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. Subscriber lists provided to directory services and to emergency agencies are not considered CPNI. Neither is aggregate information for groups of customers.

Compliance Officer

The Corporation appoints the General Manager as the CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Corporation is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training

The Compliance Officer shall arrange for the training of all employees on an annual basis, and more frequently as needed. Any new employee shall be trained when hired by the Corporation. The training shall include, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the Corporation is using.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Corporation's procedures for protecting CPNI and they understand the Corporation's disciplinary process for improper use of CPNI. If employees have any questions regarding the use of CPNI or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Corporation establishes a disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and includes the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination. A single incidence of an unintentional violation shall be cause for the least severe discipline while intentional and/or multiple violations shall be the cause of the most severe discipline. Termination of an employee must be approved by the Corporation's Board of Directors.

Customer Notification and Request for Approval to Use CPNI

The Corporation has not provided notification to its customers and has not asked for approval to use CPNI because the Corporation does not use CPNI outside of the areas that are allowed without customer approval. The Corporation does not share the customer's CPNI with any joint venture partner, independent contractor or any other third party. For marketing purposes, the Corporation will only mass market to all customers, or use CPNI to market only service offerings among the categories of service to which the customer already subscribes.

Authentication

The Corporation shall not disclose any CPNI until the customer has been appropriately authenticated as follows:

a) In-office visit - the customer must be personally known by the employee or the customer must provide a valid photo ID matching the customer's account information.

b) Customer-initiated call – the customer shall be authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information, the following guidelines shall be followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Corporation will continue with its routine customer care procedures.

- If the customer cannot provide all of the call detail information to address the customer's issue, the Corporation will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID if needed.

Notification of Account Change

The Corporation shall promptly notify customers whenever a change is made to the customer's address of record. The notification will be made by the Corporation and sent to the customer's old address of record.

The Corporation shall institute a process for tracking when a notification is required and for recording when the notification is made. Customer billing software will be used for these processes.

Definition of a CPNI Breach

A breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at http://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Miscellaneous

The Company's CPNI policies include reasonable measures to discover and protect against activity that is indicative of pretexting. Employees are instructed to notify the CPNI Compliance Officer if any such activity is suspected.

Annual Certification

The Compliance Officer will complete and – if necessary – file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

Record Retention

The Corporation shall retain all information regarding CPNI. Following are the minimum retention periods we have established:

- CPNI notification and records of approval if used – five years
- Marketing campaign if used – one year
- Breaches – five years
- Annual certification – five years
- Employee training certification – five years
- All other information – two years